APHIS DESKTOP COMPUTER SECURITY POLICY

1. PURPOSE

This Directive establishes APHIS policy for the security of APHIS-owned desktop computers.

2. REFERENCES

a. Federal Information Security Management Act (FISMA) of 2002.

b. National Institute of Standards and Technology (NIST) Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for Information Technology (IT) Professionals: A NIST Security Configuration Checklist.

c. United States Department of Agriculture (USDA) Windows XP Professional Security Assessment Guide, dated April 15, 2004.

d. APHIS Directive 3120.2, APHIS Computer Naming Conventions, dated 2/10/04.

e. APHIS Desktop Computer Security Configuration Standards.

f. APHIS Approved Desktop Software List.

3. AUTHORITIES

a. Reference 2.a. states that the Secretary of Commerce is responsible for establishing and mandating standards, guidelines, and minimum requirements for Federal information systems, based on standards developed by the NIST. Reference 2.a. also says that the head of an agency may employ information security standards which are *more* stringent than those mandated by the Secretary of Commerce, but they must contain at least the applicable standards made compulsory by the Secretary.

b. Reference 2.b. contains the NIST recommendations for securing the Windows XP operating system.

c. Reference 2.c. is to be used by all USDA agencies as a guideline to ensure a secure desktop platform. It is the assessment tool that will be used during an Office of the Inspector General or USDA Office of the Chief Information Officer audit to assess compliance to the NIST guidelines for a secure system. Reference 2.c. is in compliance with reference 2.b.

d. Reference 2.d. establishes APHIS policy for naming all computers.

e. This Directive supports and complies with references 2.a., b., c. and d. except for areas addressed by approved waivers.

4. SCOPE

This Directive applies to all APHIS-owned desktop personal computers (PCs) and their users. This Directive does not apply to servers, nor does it apply to desktop computers with a Unix-based operating system.

5. DEFINITIONS

a. **Desktop computer.** Any PC whose operating system is a Microsoft desktop operating system, e.g. Windows 2000, Windows XP or Windows XP Tablet Edition. Includes all form factors (rackmount, tower, small form factor, laptop, tablet).

b. **Server**. Any computer whose operating system is a server operating system, e.g. Windows 2000 Server, Windows 2003 Server, AIX, Linux, Mac OS Server. Includes all form factors (rackmount, tower, small form factor, laptop, tablet).

c. **APHIS Approved Desktop Software List.** A list of software approved for use on all APHIS desktop computers.

d. **Program Unit Approved Desktop Software List.** A list of software approved for use on Program Unit computers. The combined APHIS Approved Desktop Software List and Program Unit Approved Desktop Software List effectively constitute the total list of software authorized for use on any APHIS-owned computer.

6. POLICY

a. APHIS supports and enforces a policy of secure desktop computing which ensures both a secure desktop infrastructure and the continuing ability of all APHIS business units to fully support the APHIS mission. Standardized desktop configuration, an important component of the Agency's security strategy, is essential to:

(1) Ensure compliance with the requirements of Section 2.a. through d. above,

(2) Support the security certification and accreditation process for Agency desktop computers, and

(3) Achieve economies in systems management.

b. Employee awareness and adoption of security best practices also are an important cornerstone of the Agency's desktop security plan and as such:

(1) Every APHIS-owned desktop computer will conform to the configuration settings specified in Section 2.e.

(2) Every APHIS-owned desktop computer will have an authorized APHIS standard disk image and/or configuration as its base configuration. Adjustments may be made to this base configuration, including the installation of additional software, but may not alter the configuration settings specified in Section 2.e.

(3) Every APHIS-owned desktop computer will be named as mandated by Section 2.d.

(4) Every APHIS-owned desktop computer which connects to the APHIS network (i.e., receives and uses an APHIS Internet Protocol (IP) address) will be a member of one of the following APHIS domains: Windows Engineering (WE), Emergency Programs (EP), or International (INTL).

(5) Access to every APHIS-owned desktop computer will be physically restricted to minimize the opportunity for theft, destruction, tampering, or access by unauthorized persons.

(6) Decisions about which users will be granted administrative privileges to APHIS-owned computers will be made by APHIS Program Units. Each Program Unit will develop, document, and maintain an IT Administrative Privileges Guideline which establishes Program Unit policy in this area,

including the process by which these decisions are made. APHIS supports the security principle of Least Privilege, and all Program Unit policies will incorporate and support this principle in their Administrative Privileges Guideline and practices.

(7) Appropriate measures will be taken to protect data files from theft, destruction, tampering, or access by unauthorized persons, including password protection and backup.

(8) Computer event logs will be audited and monitored on a regular basis as part of an overall strategy of security risk assessment and prevention. Each Program Unit will develop, document, and maintain a Program Unit Desktop Security Monitoring Guideline which establishes Program Unit policy and practices in this area. This Guideline will include both a regular, sampled approach to event log monitoring, as well as a prescribed approach in cases of suspected or attempted security breaches.

c. Exceptions to the terms of this Directive must be approved in writing. The procedure for the Desktop Security Exception Process is described in Attachment 1, APHIS Desktop Security Exception Request (DSER).

7. RESPONSIBILITIES

a. The APHIS Chief Information Officer will:

(1) Approve and ensure implementation of this Directive.

(2) Approve any modifications to this Directive.

(3) Review and approve/deny all DSERs within 30 days of submission.

b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:

(1) Disseminate this Directive to their respective staffs.

(2) Ensure that the terms of this Directive are followed within their Program Units.

(3) Assist in promptly identifying, investigating, and helping to rectify violations of this Directive.

c. The APHIS Information Systems Program Manager (ISSPM) will:

(1) With the Customer Service Branch (CSB) Manager, Marketing and Regulatory Programs Business Services (MRPBS), Information Technology Division (ITD), design, implement, and manage a program for monitoring Agency desktop computers for compliance with the terms of this Directive.

(2) Independently, or in partnership with the CSB Manager, MRPBS, ITD, work with the Program Units to bring noncompliant computers and their users into compliance. In cases of continued noncompliancy, the ISSPM will:

(a) Take appropriate measures to deny APHIS network and resource access to computers not compliant with this Directive.

(b) Report incidents of noncompliance with this Directive to the appropriate Deputy Administrator for rectification.

(3) Review and provide recommendations for approval or denial on all DSERs.

d. The Information System Security Manager (ISSM) for each Program Unit will:

(1) Develop, maintain, and approve the Program Unit IT Administrative Privileges Guideline.

(2) Develop, maintain, and approve the Program Unit Approved Desktop Software List.

(3) Develop, maintain, and approve the Program Unit Desktop Security Monitoring Guideline.

(4) Review, provide recommendation for approval or denial of, and maintain records of, all DSERs originating from his/her Program Unit.

e. The CSB Manager, MRPBS, ITD, will:

(1) Work cooperatively with the program units to design, implement and manage an educational program for both new and existing employees to ensure awareness of APHIS desktop security practices and requirements.

(2) With the ISSPM, design, implement, and manage a program for monitoring Agency desktop computers for compliance with the terms of this Directive.

(3) Independently, or in partnership with the ISSPM, work with the program units to bring noncompliant computers and their users into compliance. In cases of continued noncompliancy, the CSB Manager will:

(a) Take appropriate measures to deny APHIS network and resource access to computers not compliant with this Directive.

(b) Report incidents of noncompliance with this Directive to the appropriate Deputy Administrator for rectification.

(4) Be responsible for approval of changes to Section 2.e.

f. The Policy, Planning and Training (PPT) Staff Manager, MRPBS, ITD, CSB, will:

(1) Maintain this Directive, including receiving requests for, and executing, modifications in response to change requests and/or new requirements.

(2) Work cooperatively with program units to manage the development and maintenance of APHIS standard disk images and/or configurations which conform to the terms of this Directive.

(3) Develop and maintain the APHIS Approved Desktop Software List.

(4) Work cooperatively with program units to develop and manage the Desktop Configuration Management Process for the Agency.

(5) Manage the APHIS DSER process for the Agency. He/she will:

(a) Receive DSERs.

(b) Review and provide technical analysis and recommendation for approval or denial on all DSERs.

(c) Maintain records of all (approved and denied) DSERs.

(6) Be responsible for maintenance of the APHIS Desktop Computer Security Configuration Standards. He/she will:

(a) Receive requests for modification.

(b) Respond to requests for modification and/or new requirements within 30 days of request or notification of new requirement.

(c) Provide a forum for discussion among all program units and appropriate members of MRPBS, ITD, TRM, of proposed changes prior to approval.

(d) Notify all IT employees of changes within 14 days of the change.

(e) Publish in a centrally and electronically accessible location.

g. Agency Computer Support Employees will:

(1) Comply with the terms of this Directive when configuring desktop computers.

(2) Take immediate corrective action to bring computer configurations into conformance with the terms of this Directive or obtain an approved APHIS DSER for nonconforming configuration elements for computers under their care.

(3) Assist in promptly identifying, investigating, and helping rectify violations of this Directive.

(4) Assist users in understanding, acquiring, and using appropriate backup techniques and strategies to prevent data loss.

(5) Monitor Event Logs as defined in their Program Unit Desktop Security Monitoring Guideline.

(6) Provide input concerning desktop configurations and standards established in this Directive and Section 2.e., including:

(a) Requests for modifications,

(b) Testing in program unit environments,

(c) Collaboration on strategies which meet external security requirements,

(d) Effective security of the Agency's desktop environment, and

(e) Support of APHIS employees in performing mission tasks.

h. APHIS employees will:

(1) Ensure that the terms of this Directive are followed.

(2) Ensure that any APHIS-owned desktop computer which they use, or for which they have support responsibility, conforms to the terms of this Directive or obtain an approved DSER for nonconforming configuration elements.

(3) Report suspicious activity and/or suspected computer security breaches to appropriate Agency security employees via approved reporting processes.

(4) Use appropriate backup techniques and strategies to prevent loss of their data files.

8. INQUIRIES

a. Questions concerning the information and processes described in this Directive should be directed to the PPT Staff Manager, MRPBS, ITD, CSB.

b. This Directive can be accessed via the Internet APHIS website at ***www.aphis.usda.gov/library***

/s/
Tracy Bowman
Acting APHIS Chief Information Officer